ABSTRACT OF THE DISCLOSURE

The present invention relates to a method of detecting malicious scripts using a code insertion technique. The method of detecting malicious scripts according to the present invention comprises the step of checking values related to each sentence belonging to call sequences by using method call sequence detection based on rules including matching rules and relation rules, wherein the checking step comprises the steps of inserting a self-detection routine (malicious behavior detection routine) call sentence before and after a method call sentence of an original script, and detecting the malicious codes during execution of the script through a self-detection routine inserted into the original script. According to the present invention, since a detection routine is configured to operate during the execution of scripts, dynamically determined parameters and return values can be checked and thus detection accuracy can be improved. Further, since codes are inserted into only the scripts entering from the outside, unnecessary overhead is not generated. Furthermore, since the modified codes perform the self-detection even in systems in which additional anti-viruses are not installed, there is an advantage in that the propagation of malicious scripts can be suppressed.